



# Best Practices for Breeze Directory Service Integration

## Trademarks

1 Step RoboPDF, ActiveEdit, ActiveTest, Authorware, Blue Sky Software, Blue Sky, Breeze, Breezo, Captivate, Central, ColdFusion, Contribute, Database Explorer, Director, Dreamweaver, Fireworks, Flash, FlashCast, FlashHelp, Flash Lite, FlashPaper, Flex, Flex Builder, Fontographer, FreeHand, Generator, HomeSite, JRun, MacRecorder, Macromedia, MXML, RoboEngine, RoboHelp, RoboInfo, RoboPDF, Roundtrip, Roundtrip HTML, Shockwave, SoundEdit, Studio MX, UltraDev, and WebHelp are either registered trademarks or trademarks of Macromedia, Inc. and may be registered in the United States or in other jurisdictions including internationally. Other product names, logos, designs, titles, words, or phrases mentioned within this publication may be trademarks, service marks, or trade names of Macromedia, Inc. or other entities and may be registered in certain jurisdictions including internationally.

## Third-Party Information

This guide contains links to third-party websites that are not under the control of Macromedia, and Macromedia is not responsible for the content on any linked site. If you access a third-party website mentioned in this guide, then you do so at your own risk. Macromedia provides these links only as a convenience, and the inclusion of the link does not imply that Macromedia endorses or accepts any responsibility for the content on those third-party sites.

**Copyright © 2005 Macromedia, Inc. All rights reserved. This manual may not be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form in whole or in part without written approval from Macromedia, Inc. Notwithstanding the foregoing, the owner or authorized user of a valid copy of the software with which this manual was provided may print out one copy of this manual from an electronic version of this manual for the sole purpose of such owner or authorized user learning to use such software, provided that no part of this manual may be printed out, reproduced, distributed, resold, or transmitted for any other purposes, including, without limitation, commercial purposes, such as selling copies of this documentation or providing paid-for support services.**

## Acknowledgments

Project Management: Stephanie Gowin, Suzanne Smith,

Writing: Tom Wetzel

Editing: Geta Carlson

Production Management: Patrice O'Neill

Media Design and Production: Adam Barnett, John Francis, Mario Reynoso

First Edition: July 2005

Macromedia, Inc.  
601 Townsend St.  
San Francisco, CA 94103

# Contents

<b>Best Practice for Breeze Directory Service Integration . . . . .</b>	<b>5</b>
Working with LDAP . . . . .	6
Importing users . . . . .	6
Importing groups . . . . .	8
Selecting the directory node to be imported . . . . .	9
Importing sub-branches . . . . .	11
Internal (nonimported) versus external (imported) users and groups . . . . .	11
Working with branches in Directory Service . . . . .	12
Managing passwords . . . . .	14
Automatic single sign-on . . . . .	14
Making manual changes in the Breeze configuration . . . . .	15
NTLM authentication . . . . .	16
HTTP header-based authentication . . . . .	17
Other methods for managing passwords . . . . .	17
Notifying users to set their password . . . . .	17
Setting the password to an LDAP attribute . . . . .	18
Recommended practices for synchronization . . . . .	18
Scheduling synchronizations . . . . .	18
Verifying connections to the LDAP server . . . . .	19
Log file format . . . . .	20
Previewing the synchronization . . . . .	21
Questions about Breeze Directory Service Integration . . . . .	22



# Best Practice for Breeze Directory Service Integration

[Working with LDAP](#) ..... 6

[Managing passwords](#) ..... 14

[Recommended practices for synchronization](#) ..... 18

[Questions about Breeze Directory Service Integration](#) ..... 22

Macromedia Breeze Directory Service Integration (DSI) allows enterprise customers to incorporate users and groups into Macromedia Breeze from existing directories using Lightweight Directory Access Protocol (LDAP). LDAP is an Internet client-server protocol used for lookup of user contact information from an LDAP-compliant directory server. DSI supports the following directory servers:

- Microsoft Active Directory (Windows 2003 server)
- Sun One Directory Server 5.2
- Open LDAP 2.2.23
- Novel eDirectory 8.7.3
- IBM Directory Server 5.1

DSI enables the Breeze server to connect as an LDAP client to an LDAP directory, import users and groups, and ensure that information about these imported users and groups in the Breeze database is kept in sync with the external LDAP directory.

With DSI, administrators can avoid having to manually add users to Breeze one by one. User accounts are created automatically in Breeze through manual or scheduled synchronizations with an organization's directory service. The best solution is to combine DSI with a system for authenticating users which allows automatic single sign-on for Breeze. A user who is logged on to their desktop using their network user name and password can access Breeze services directly, bypassing the Breeze login screen.

To perform a directory integration task, you must be defined as an administrator in your Breeze profile. An administrator is defined in the Create Administrator screen of the Application Management Console. The administrator's point of access for Breeze DSI is the Directory Service Settings tab in the Application Management Console. Setting up and initiating synchronization with an LDAP server is accomplished with the screens accessible through this tab.

## Working with LDAP

Users and groups in a directory are LDAP called *entries*. Each entry is a collection of attributes that has a name, called a *distinguished name* (DN). The attribute values for user entries consists of user information such as phone number, e-mail address, and photo. The DN describes a path to the entry through a hierarchical tree structure.

The DN that refers to a particular entry in the LDAP directory is formed by taking the name of the entry itself (called a *relative distinguished name*, RDN) and concatenating it with the names of its ancestor entries in the tree structure. The way that the tree structure is organized may reflect geographical locations or departmental boundaries within an organization. For example, if Alicia Solis is a user in the QA department of Acme, Incorporated in France, the DN for this user might be:

```
cn=Alicia Solis, ou=QA, c=France, dc=Acme, dc=com
```

The DN specifies the path through the tree to the user from the root. In the example above, the root is specified by `dc=com`. Each of the attributes that make up an entry has a type and one or more values. The values for an attribute depend on what type of attribute it is. Mnemonic strings are used to specify types, such as `ou` for organizational unit or `cn` for common name, as in the example above.

## Importing users

When importing user entries from an LDAP server, the administrator uses the User Profile Mapping screen to map Breeze user profile fields to the equivalent attribute in the LDAP entries. The following example shows a mapping of an LDAP user entry to a Breeze user profile:

```
Login: sAMAccountName  
First Name: givenName  
Last Name: sn  
Email: userPrincipalName  
Network Login: sAMAccountName
```

Macromedia Breeze

Application Settings | **Directory Service Settings**

LDAP Settings | Synchronization Settings | Synchronization Actions | Synchronization Logs

Connection Settings | **User Profile Mapping** | Group Profile Mapping

### User Profile Mapping

Macromedia Breeze will synchronize the following user profile fields with the corresponding fields in your Directory Service. Please specify the field names as they exist in your Directory Service. If you wish to activate a user field in Breeze, please click [here](#).

If you have set the Login Policy to use the e-mail address as the login, the Breeze login and e-mail fields must map to the same directory service field. [Edit Login Policy](#)

Macromedia Breeze User Field Name	Directory Service Field Name
Login*	sAMAccountName
First Name*	givenName
Last Name*	sn
E-mail*	userPrincipalName
Network Login	sAMAccountName

\* - indicates required fields

Search for users in these branches:

Add

The required fields are: Login, First Name, Last Name, and Email. If you have defined any custom fields (Breeze Administration > Users and Groups > Customize User Profile), these fields are added to the User Profile Mapping screen. In the example above Network Login is a custom field.

# Importing groups

To map LDAP group entry attributes to Breeze group profiles, the administrator creates a mapping on the Group Profile Mapping screen. The following shows an example of a mapping between LDAP group entry attributes and a Breeze group profile:

Name: cn

Membership: member

Name and membership are the two required fields for Breeze group profiles. Breeze group profiles do not support custom fields, unlike the Breeze user profiles.

Group Profile Mapping - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Links

Macromedia Breeze

Application Settings Directory Service Settings

LDAP Settings Synchronization Settings Synchronization Actions Synchronization Logs

Connection Settings User Profile Mapping Group Profile Mapping

Group Profile Mapping

Macromedia Breeze will synchronize the following group profile fields with the corresponding fields in your Directory Service. Please specify the field names as they exist in your Directory Service.

Macromedia Breeze User Field Name	Directory Service Field Name
Group Name*	cn
Group Member*	member

\* - indicates required fields

Search for groups in these branches:

Add

Done My Computer

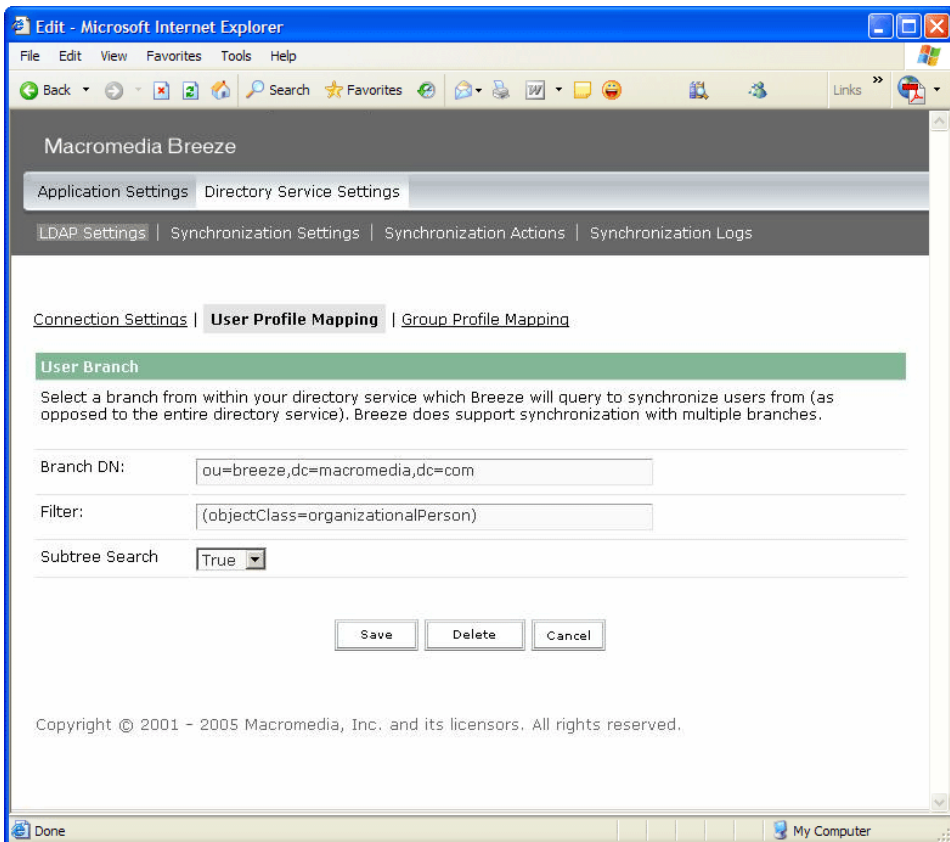


## Selecting the directory node to be imported

When importing users and groups from an LDAP directory into Breeze, you specify a path to a section of the LDAP tree by using the DN. This specifies the scope of the search of the LDAP directory for selection of entries. You can restrict the selection of entries within that part of the tree by using a filter to specify a condition that an entry must satisfy to be selected. For example, if the filter specifies

`(objectClass=organizationalPerson)`

then only entries that have the attribute `organizationalPerson` are selected for import. The example below shows the User Branch editor which you use to specify the user branch DN.



The attribute `objectClass` must be present in every entry in a LDAP directory. This attribute defines the rules and required attributes for that entry.

There are two ways of relating group and user entries in LDAP directories. A directory may be configured with the user groups under the same node in an LDAP branch. In that case, the user and group settings for importing entries contain the same branch DN. This means you must use a filter to select only the users when importing users and a filter to select only groups when importing groups.

The second type of LDAP tree structure puts users and groups under different branches in the tree. In this case, when you import the users you use a branch DN that selects the user branch. When you import groups, you use a branch DN that selects the groups branch.

Separate administration screens for selecting users and groups to be imported from the LDAP server are provided in the Breeze Directory Service Settings tab. For example, administrators use the Group Branch editor, shown below, to select groups for import:

The screenshot shows a web browser window titled "Edit - Microsoft Internet Explorer" displaying the Macromedia Breeze administration interface. The "Directory Service Settings" tab is active, and the "Group Profile Mapping" sub-tab is selected. The "Group Branch" section contains the following fields:

- Branch DN:**
- Filter:**
- Subtree Search:**

Below the fields are three buttons: "Save", "Delete", and "Cancel". At the bottom of the page, a copyright notice reads: "Copyright © 2001 - 2005 Macromedia, Inc. and its licensors. All rights reserved."

## Importing sub-branches

Let us suppose that you have set the Branch DN on the User Profile Mapping screen to import all the users in a certain branch of the directory tree. In that case, there may be sub-branches below that level in the tree structure. For example, you may set the branch to import all employees in the sales department by setting the branch DN, as follows:

```
ou=Sales, dc=Acme, dc=com
```

But this branch of the tree may have the employees of sales offices in sub-branches. In that case, DSI will import the users from the sub-branches below that level in the tree if you set the Subtree Search parameter to true.

## Internal (nonimported) versus external (imported) users and groups

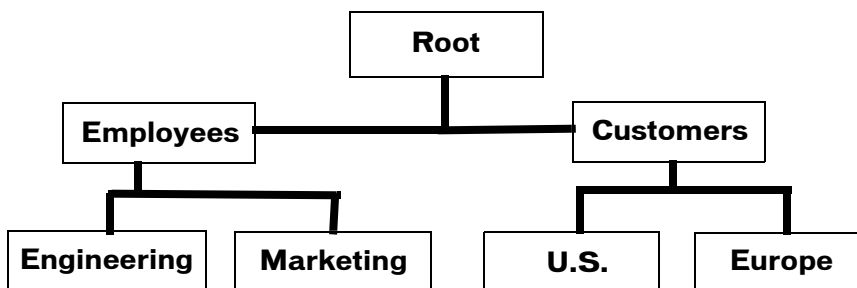
You may want to have some users or groups within Breeze that are not imported from the external LDAP server. For this reason, the Breeze database makes a distinction between internal and external Breeze users and groups. Users or groups that have been created directly in Breeze and not imported from an LDAP directory using DSI are *internal*. Any user or group that has been imported into the Breeze database using Directory Service is *external*.

To ensure that imported groups are kept in sync with the external LDAP directory, the membership of external groups can be changed only through DSI. Internal Breeze users and groups cannot be added to external groups. However, external users and groups can be added to internal groups in Breeze. For example, if you want to add all the users in the Singapore office to a Breeze Presentation user group, they can be assigned to the internal Breeze group even if it has other users that have not been imported through DSI.

If the value of the login or name of an imported user or group entry matches the Breeze login for an existing internal Breeze user or group, Breeze DSI will change that user or group from internal to external and log a warning to the scynchronization log.

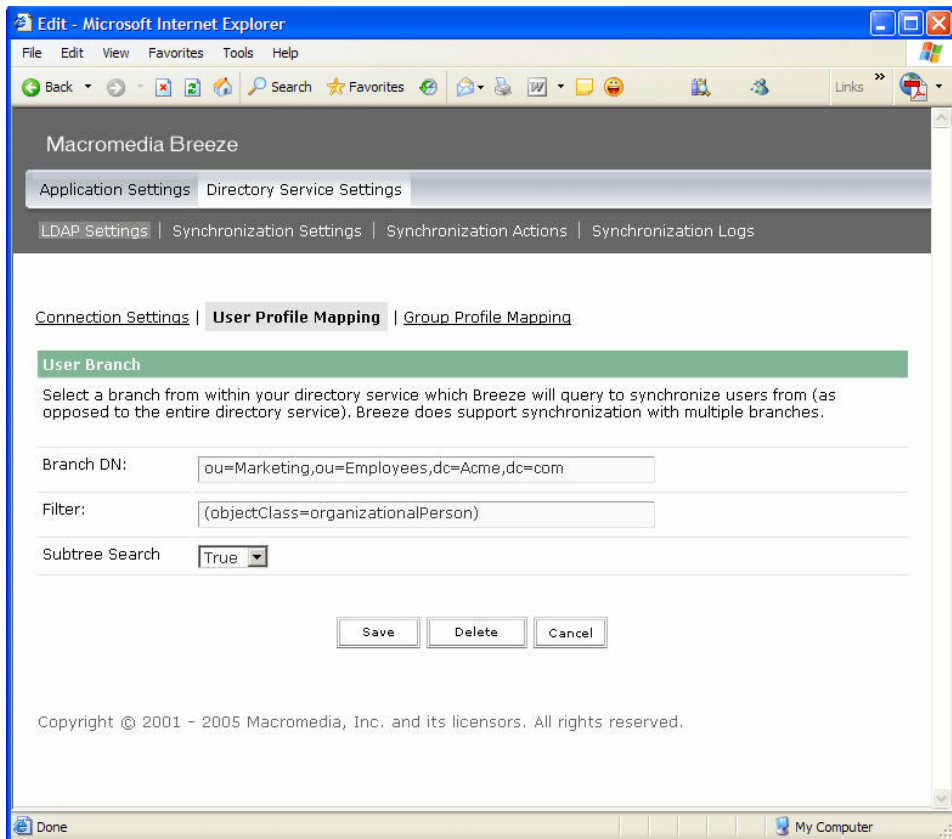
## Working with branches in Directory Service

When importing users and groups from an LDAP-compliant directory into the Breeze directory, you may want to import only the users of a particular group within your organization. To do this, you need to know where the entries for that group are located within the directory tree structure. This depends on the particular topology or tree structure in the directory you are importing from. LDAP allows a number of different possible arrangements. One possible arrangement is shown below.



A common technique is to use the organization's Internet domain as the root for the tree structure. A company might then use `dc=com` to specify the root element in the tree. A DN that specifies the Singapore sales office for Acme, Inc. might then be: `ou=Singapore, ou=Marketing, ou=Employess, dc=Acme, dc=com`. In this example, `ou` is an abbreviation for organizational unit, and `dc` is an abbreviation for domain component. In the Breeze Directory Service tab, there are separate screens for specifying the branch DN for import of users and import of groups.

The User Branch editor, shown below, is used to select the users for import. The Marketing node from the above example is selected in this screen.



When you map Breeze user profiles to LDAP fields, the Add Branch DN button on the User Profile Mapping screen enables you to specify a branch DN to select the users to be imported to the Breeze directory. When you map a Breeze group profile on the Group Profile Mapping screen, there is also an Add Branch DN button that allows you to select a branch DN for the import of groups to the Breeze directory.

Not all LDAP directories have a single root. You can handle this by defining separate branches to be imported.

# Managing passwords

When Breeze imports user information using DSI, this does not provide Breeze with access to the user's network password. In theory, an organization could use an LDAP field to store the user password in the directory. But storing user passwords in clear text would be a major security breach. Because Breeze DSI does not obtain the network password for users, some other method for managing passwords for users imported into the Breeze directory from external LDAP servers is needed. Several methods for doing this are discussed below.

## Automatic single sign-on

The recommended method for managing Breeze user passwords and authentication with DSI is to use it with automatic single sign-on. Automatic single sign-on is a mechanism that allows a user who is logged in to gain access to Breeze and resources for which they have permission without being prompted each time for their login and password.

Two methods for implementing automatic single sign-on are supported for Breeze:

- Windows NT LAN Manager (NTLM) authentication
- HTTP header-based authentication

If you plan on using either of these methods for single sign-on authentication, you will want set the authentication policy for DSI to Do Nothing in the DSI Policy Settings screen, as shown below.

The screenshot shows the Macromedia Breeze web interface. At the top, there's a header bar with 'Macromedia Breeze' and a navigation menu with 'Application Settings', 'Directory Service Settings' (selected), 'LDAP Settings', 'Synchronization Settings', 'Synchronization Actions', and 'Synchronization Logs'. Below the navigation, there's a sub-menu with 'Schedule Settings' and 'Policy Settings' (selected). The main content area has a green header for 'Password Setup Policy'. The text below states: 'This policy determines how the synchronization should set up passwords for new users.' There are three radio button options: 1. 'Do nothing. - Use this option if you have integrated Breeze with an external authentication system and do not need to set up passwords during synchronization.' (This is selected). 2. 'Send a link to set the password. - Use this option if you need to set up passwords and all users have e-mail addresses. They will receive an e-mail with a link to set their password.' 3. 'Set the password to the value of an LDAP attribute. - Use this option if you need to set up passwords and some users do not have e-mail addresses. Their initial password will be set to the value of this LDAP attribute in their directory service entry. Password validation policies will not be applied to this initial value.' Below these options is a text input field labeled 'LDAP Attribute:'. The next section has a green header for 'Deletion Policy' and a checked checkbox with the text 'Delete users and groups in Breeze that have been deleted from your directory service'. At the bottom, there are 'Save' and 'Cancel' buttons.

Macromedia Breeze

Application Settings | **Directory Service Settings** | LDAP Settings | Synchronization Settings | Synchronization Actions | Synchronization Logs

Schedule Settings | **Policy Settings**

**Password Setup Policy**

This policy determines how the synchronization should set up passwords for new users.

- ☒ Do nothing. - Use this option if you have integrated Breeze with an external authentication system and do not need to set up passwords during synchronization.
- ☐ Send a link to set the password. - Use this option if you need to set up passwords and all users have e-mail addresses. They will receive an e-mail with a link to set their password.
- ☐ Set the password to the value of an LDAP attribute. - Use this option if you need to set up passwords and some users do not have e-mail addresses. Their initial password will be set to the value of this LDAP attribute in their directory service entry. Password validation policies will not be applied to this initial value.

LDAP Attribute:

**Deletion Policy**

☒ Delete users and groups in Breeze that have been deleted from your directory service

## Making manual changes in the Breeze configuration

Implementing either NTLM or HTTP header-based authentication requires that you make manual changes in the Breeze custom.ini file. It is recommended that this be done only by an experienced Breeze administrator with guidance from Breeze technical support.

### To set Breeze configuration variables manually for authentication integration:

1. Stop all Breeze services.
2. Enter the new parameters and values (as described in the following sections).
3. Save the modified file as custom.ini.
4. Restart all Breeze services.
5. Verify that the Breeze services are functioning successfully.

## NTLM authentication

NTLM is a challenge/response protocol that enables a client to prove its identity without providing a password. An application queries an authentication server for the user's credentials. The NTLM routine is transparent to the user. To implement NTLM for Breeze, you will need to add the following parameters to the Breeze custom.ini file:

```
NTLM_DOMAIN=domain
```

```
NTLM_SERVER=NTLM_server_IP_address
```

where *domain* is the name of the domain, such as acme.com, and *NTLM\_server\_IP\_address* is the IP address of the NTLM authentication server. The numeric IP address must be used with NTLM\_SERVER; the host name won't work.

Breeze and Microsoft NTLM use different login policies for authenticating users. These policies must be made consistent before a user can employ single sign-on to access Breeze. By default, Breeze employs the user's e-mail address (alfred\_smith@acme.com) and password as the primary login to authenticate the user. But you can configure Breeze to use an external login, such as a user name and password for authentication.

The Breeze login and password policy is configured in Breeze Manager (Administration > Edit Login and Password Policies). In the Login Policy section you can specify whether to use the user's e-mail login as the default login to Breeze. Select No if you want Breeze to accept a user name as the authentication vehicle. This configuration makes the Breeze password policy consistent with the NTLM password policy.

In order for users to make use of single sign-on with NTLM authentication, they must be using Internet Explorer. Other web browsers do not support NTLM authentication.



## HTTP header-based authentication

HTTP header-based authentication uses extra fields in the header of an HTTP request for authentication of the user. In this scenario, Breeze login requests are routed to a proxy server positioned between the client and the Breeze Server. The proxy server performs the role of the authentication server. The proxy server takes the original HTTP request from the client and augments it with an extra HTTP header field with the user ID. The Breeze server uses this information to identify the user. If the user passes this authentication test, the Breeze server creates a valid session and allows the user to begin using the system.

To implement HTTP header-based authentication for Breeze, changes must be made to two Breeze configuration files.

1. Access the Breeze server and open the following file:

*Breeze\_Install\_Dir\appserv\conf\WEB-INF\web.xml*

Change the following section to enable it by removing the commenting-out code:

```
<!--
  <filter-mapping>
    <filter-name>HeaderAuthenticationFilter</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
-->
```

1. Add an entry to the Breeze custom.ini file as follows:

`HTTP_AUTH_HEADER=header_field_name`

where *header\_field\_name* is the extra HTTP field used for authentication. For example:

`HTTP_AUTH_HEADER=X-User-Id`

The value of this field must be the user login that already exists in Breeze.

## Other methods for managing passwords

If you select not to use automatic single sign-on, there are two other methods available for managing passwords with DSI. Under both of these scenarios, users will need to enter their Breeze login and password.

### Notifying users to set their password

In this scenario, users who are added to Breeze through DSI are automatically sent an e-mail with a link to set their password. This option can be selected on the Policy Settings screen under the Directory Service Settings tab.

## Setting the password to an LDAP attribute

Under this scenario, DSI would set the initial password of imported users to the value of an attribute in the directory entry for that user. For example, if the LDAP directory contains the employee ID number as a field, you could set the initial password for users to their employee ID number. After users log in using this initial password, they can change their passwords.

## Recommended practices for synchronization

An administrator can initiate two different kinds of synchronization of Breeze with the external LDAP directory:

- A manual synchronization that immediately synchronizes the Breeze directory with the organization's LDAP directory.
- Scheduled synchronization that takes place at defined intervals.

Some directory servers have limits on the number of entries that can be imported with a single query. If you cannot remove this limit or do not want to remove the limit due to directory server performance issues, you can work around the limit by separately synchronizing to the various branches that make up the directory tree for your organization. Paging—packaging multiple queries into one request—is not supported by Breeze DSI. Another solution for limits on directory request size for the Active Directory is to increase the page size. But this might have an adverse impact on directory server performance.

Macromedia recommends the following practices for synchronization.

## Scheduling synchronizations

An initial synchronization of the Breeze directory with the external LDAP directory might consume significant resources if you are importing a large number of users and groups. If this is the case, Macromedia recommends that you do the initial synchronization at an off-peak time, such as late at night. You may also want to do the initial synchronization manually.

You could do all of the subsequent synchronizations manually also, but the recommended practice is to use scheduled synchronizations to ensure that Breeze has an up-to-date picture of the users and groups imported from the organization's LDAP directory service. You use the Schedule Settings screen (shown below) to set this up.

If you anticipate relatively few changes of LDAP server entries between scheduled synchronizations, you may not need to worry about the timing of the scheduled synchronization. But if a significant number of changes are possible—perhaps because of the large scope of the organization that is being synchronized—you may also want to schedule the synchronizations at an off-peak time in order to minimize impact on users.

When a synchronization takes place, Breeze DSI only imports those entries in its scope of search that have changed in the content of at least one of its fields, when compared to the existing entry in the Breeze directory.

The screenshot shows the Macromedia Breeze web interface. At the top, there's a header bar with "Macromedia Breeze" and a navigation menu with "Application Settings", "Directory Service Settings", "LDAP Settings", "Synchronization Settings", "Synchronization Actions", and "Synchronization Logs". Below this, there's a sub-navigation bar with "Schedule Settings" and "Policy Settings". The "Schedule Settings" section is highlighted in green. It contains a description: "Macromedia Breeze will synchronize users with your Directory Service based on the settings below. Scheduling synchronizations at off-peak hours is recommended to ensure optimal end-user experiences." Below the description, there's a checkbox labeled "Enable scheduled synchronization" which is checked. Underneath, it says "Perform synchronization at the following times:". There are two input fields: "Start time:" with a dropdown menu showing "1", "June", "2005", and "01:00 AM"; and "Synchronization Interval:" with a dropdown menu showing "Daily". At the bottom, there's a "Save" button.

## Verifying connections to the LDAP server

The Connection Settings screen in the Breeze console asks you for information needed to connect to the LDAP server (such as the server's URL). Before you attempt to do an initial synchronization, importing users and groups into the Breeze server database, Macromedia recommends that you verify the parameters you are using for connection to the LDAP server. Open-source LDAP browsers are available to carry out this task. For example, LDAP Editor/Browser can be downloaded from the following site: [www-unix.mcs.anl.gov/~gawor/ldap/](http://www-unix.mcs.anl.gov/~gawor/ldap/)

## Log file format

The synchronization logs store values in a comma-separated format. In the tables below *principal* refers to user and group entries. The following values are included in the log entries:

Field	Description
Date	Formatted date/time value, with time to the millisecond. The format is yyyyMMdd'T'HHmmss.SSS.
Principal ID	Breeze login or group name.
Principal type	A single character, U for user, G for group.
Event	The action taken or condition encountered.
Detail	Detailed information about the event.




The following table describes the different kinds of events that can appear in the synchronization log files:

Event	Description	Detail
add	The principal was added to Breeze.	Abbreviated XML packet describes the updated fields. A series of <code>&lt;fieldname&gt;value&lt;/fieldname&gt;</code> . The parent node and non-updated fields are omitted. For example: <code>&lt;first-name&gt;Joe&lt;/last-name&gt;</code>
update	The principal exists as an external user in Breeze, and some fields were updated.	
update-members	The principal exists as an external group in Breeze, and principals were added to or removed from membership in the group.	Abbreviated XML packet that describes the added and removed members. The parent node is omitted: <code>&lt;add&gt;ID list&lt;/add&gt;</code> <code>&lt;remove&gt;ID list&lt;/remove&gt;</code> The <code>ID list</code> is a series of <code>&lt;id&gt;principal ID&lt;/id&gt;</code> packets where <i>principal ID</i> is an ID that would be listed in the Principal ID column, such as a user login or group name. If there are no members of an ID list, the parent node is output as <code>&lt;add/&gt;</code> or <code>&lt;remove/&gt;</code> .
delete	The principal was deleted from Breeze.	

Event	Description	Detail
up-to-date	The principal exists as an external principal in Breeze and is already synchronized with the external directory. No changes were made.	A user or group created in Breeze is considered an internal principal. A user or group created by the synchronization process is considered an external principal.
make-external	The principal exists as an internal principal in Breeze and was converted to an external principal.	This event permits the synchronization to modify or delete the principal and is usually followed by another event that does one or the other. This event is logged in the warning log.
warning	Some other warning-level event occurred.	Warning message.
error	An error occurred.	Java exception message.

## Previewing the synchronization

Before you try to import users and groups in an initial synchronization, it is also recommended that you first preview the synchronization. A preview is a kind of dry run to test the mappings you are using, and to ensure that there are no errors. In a preview, errors are logged but no actual import of users and groups takes place. The log file that is generated can help you to diagnose any problems in the synchronization. You can access the synchronization logs through the Synchronization Logs screen, shown below.

Macromedia Breeze			
Application Settings   Directory Service Settings			
LDAP Settings   Synchronization Settings   Synchronization Actions   Synchronization Logs			
✓	Name ▾	Type ▾	Date Modified ▾
<input type="checkbox"/>	 <a href="#">Scheduled Synchronization</a>	Archive	06/01/2005 1:00 AM
<input type="checkbox"/>	 <a href="#">Manual Synchronization</a>	Archive	05/30/2005 6:20 PM
<input type="checkbox"/>	 <a href="#">Preview Synchronization</a>	Archive	05/30/2005 6:00 PM

Logs consist of events with one line per event. The synchronization produces at least one event for each principal (user or group) processed. If any warnings or errors are generated during a preview synchronization, a second warning log listing all the warnings and errors is also generated. The administrator can use these log files to diagnose problems in the synchronization before attempting to actually synchronize the Breeze directory with the external LDAP directory.

## Questions about Breeze Directory Service Integration

- **What happens in Breeze when I delete a user in the LDAP directory?**

The action that Breeze takes depends on the deletion policy that you have selected for DSI. You can choose to have DSI delete external users in Breeze if they have been deleted from the source LDAP server. In that case, the user is deleted in Breeze if a synchronization discovers that the user has been deleted from the LDAP directory. If you disable this DSI feature on the Deletion Policy screen, a user deleted in the LDAP server is not automatically deleted from the Breeze database on the next synchronization.

- **Can I have a combination of users imported from an LDAP directory and users manually created in Breeze?**

Yes. Both internal and external users can coexist in the Breeze directory.

- **Can I integrate my corporate directory with my Application Server Provider (ASP) Breeze implementation?**

No. Under the ASP implementation of Breeze, Macromedia is the host for the Breeze services. DSI is not supported in that implementation.

- **Is there a way to populate particular Breeze groups from a particular LDAP directory group?**

Once users and groups from the LDAP group have been imported into Breeze, you can assign them to Breeze groups manually.

- **How many directory users can I import into the Breeze database?**

The number of external Breeze users is limited only by the capacity of your database. In tests, more than 100,000 user entries have been successfully synchronized with a Breeze directory using DSI. However, if you are trying to import a very large number of users (thousands of users), you may want to do this in stages, performing separate synchronizations for the various directory branches.

- **What if there is a make a mistake when importing thousands of users and I want to start over again. Can I easily remove the external users and remove them?**

If you have the deletion policy set to true, the unwanted users and groups will be automatically deleted when you do another synchronization. Another solution would be to sync Breeze with another LDAP server that doesn't have the users and groups you want to delete, and do this with the deletion policy set to true.

- **Which fields from the directory can I map to Breeze profiles? Can I automatically populate Customized User Profile fields on the Breeze server?**

Yes. The User Profile Mapping screen in DSI lets you specify customized fields that you want to map to particular LDAP entry attributes.

- **Is directory information automatically encrypted over the network when it is transferred from the LDAP server?**

No. LDAPS is not currently supported for DSI.

- **What if someone already has an account in Breeze that matches the LDAP directory account? Will that user loose all their Breeze-specific content, such as links to meetings?**

No. The existing Breeze data is not overwritten. The user is changed from an internal to external user.

